CAT- I

Cryptography and Network security

Prof. Karthika .V.

1) i) $79 . x \equiv 1 \bmod 3220$.

i	r_i	q_i	x_i	y_i
-1	3220		1	0
0	79		0	1
1	60	40	1	-40
2	19	1	$0-1$ $=-1$	$1-(-40\times1)$ $=41$
3	3	3	$1-(-1\times3)$ $=4$	$-40-(41\times3)$ $-40-123=-163$
4	1	6	$-1-(4\times6)$ $=-25$	$41-(-163\times6)$ $=41+978=1019$
5	0	3		

3220	79
-25	1019

Ans $= 1019$ $[79 . 1019 \equiv 1 \bmod 3220]$

1) ii)

$2^1 \bmod 13 = 2$

$2^2 \bmod 13 = 4$

$2^3 \bmod 13 = 8$

$2^4 \bmod 13 = 3$

$2^5 \bmod 13 = 6$

$2^6 \bmod 13 = 12$

$2^7 \bmod 13 = 11$

$2^8 \bmod 13 = 9$

$2^9 \bmod 13 = 5$

$2^{10} \bmod 13 = 10$

$2^{11} \bmod 13 = 7$

$2^{12} \bmod 13 = 1$

Yes 2 is a primitive root of 13 as all values are distinct

Discrete log table

a	1	2	3	4	5	6	7	8	9	10	11	12
$\log_{2,13}(a)$	12	1	4	2	9	5	11	3	8	10	7	6

2) i) $X \equiv 3 \pmod 7$

$X \equiv 3 \pmod 5$

$X \equiv 4 \pmod{12}$

$M = m_1 m_2 m_3 = 7 \times 5 \times 12 = 420$

$a_1 = 3$	$m_1 = 7$	$M_1 = \frac{M}{m_1} = \frac{420}{7} = 60$	$M_1^{-1} = 2$
$a_2 = 3$	$m_2 = 5$	$M_2 = \frac{M}{m_2} = \frac{420}{5} = 84$	$M_2^{-1} = 4$
$a_3 = 4$	$m_3 = 12$	$M_3 = \frac{M}{m_3} = \frac{420}{12} = 35$	$M_3^{-1} = 11$

60 mod 7

i	r_i	q_i	x_i	y_i
-1	60		1	0
0	7		0	1
1	4	8	1	-8
2	3	1	-1	9
3	1	1	2	-17
4	0	3		

60 7

2 -17

84 mod 5

i	r_i	q_i	x_i	y_i
-1	84		1	0
0	5		0	1
1	4	16	1	-16
2	1	1	-1	17
3	0	4		

84 5

-1 17

-1+5

= 4

35 mod 12

i	r_i	q_i	x_i	y_i
-1	35		1	0
0	12		0	1
1	11	2	1	-2
2	1	1	-1	3
3	0	11		

35 12

-1 3

$-1+12$

$=11$

$$X = [a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}] \bmod M$$

$$= [(3\times 60\times 2) + (3\times 84\times 4) + (4\times 35\times 11)] \bmod 420$$

$$= (360 + 1008 + 1540) \bmod 420$$

$$= 2908 \bmod 420$$

$$= 388$$

2) (ii) $a_1 = 3$, $a_2 = 4$

$m_1 = 6$ $m_2 = 8$

m_1 & m_2 are not relatively prime modulo.

3) i) Message : TCEM

$[19\ 2]\ [4\ 12]$

A	B	C	D	E	F	G
0	1	2	3	4	5	6

H	I	J	K	L	M	N	O
7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

$$K = \begin{pmatrix} 17 & 8 \\ 19 & 3 \end{pmatrix}$$

Encryption

$C = PK \bmod 26$

$$= (19\ 2)\begin{pmatrix} 17 & 8 \\ 19 & 3 \end{pmatrix} \bmod 26 = (361\ 158) \bmod 26$$

$$= (23\ 2) = (X\ C)$$

1

$C = PK \bmod 26$

$$= (4\ 12)\begin{pmatrix} 17 & 8 \\ 19 & 3 \end{pmatrix} \bmod 26 = (296\ 68) \bmod 26$$

$$= (10\ 16) = (K\ Q)$$

TCEM = XCKQ 2

Decryption

$P = CK^{-1} \bmod 26$

$$K^{-1} = \frac{1}{|K|} \text{adj } K \bmod 26 =$$

$$|K| \bmod 26 = [(17 \times 3) - (19 \times 8)] \bmod 26 = -101 \bmod 26$$

$$= \cancel{-}25 \bmod 26$$

$$= 3.$$

$$\text{Adj } K = \begin{pmatrix} 3 & -8 \\ -19 & 17 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} 3 & 18 \\ 7 & 17 \end{pmatrix}$$

$$K^{-1} = \frac{1}{3} \begin{pmatrix} 3 & 18 \\ 7 & 17 \end{pmatrix} \text{ mod } 26 \quad = 3^{-1} \text{ mod } 26.$$

2

$$= 9.$$

$$75 \text{ mod } 26 = 17$$

i	r_i	q_i	x_i	y_i
-1	75		1	0
0	26		0	1
1	23	2	1	-2
2	3	1	-1	3
3	2	7	8	-23
4	1	1	-9	26
5	0	2		

$$\boxed{-9 + 26 = 17}$$

$$K K^{-1} \text{ mod } 26$$

$$\begin{pmatrix} 17 & 8 \\ 19 & 3 \end{pmatrix} \begin{pmatrix} 1 & 6 \\ 11 & 23 \end{pmatrix}$$

$$\begin{pmatrix} 105 & 286 \\ 52 & 183 \end{pmatrix} \text{ mod } 26$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$K^{-1} = 9 \begin{pmatrix} 3 & 18 \\ 7 & 17 \end{pmatrix} \text{ mod } 26 = \cancel{\begin{pmatrix} 51 & 306 \\ 119 & 289 \end{pmatrix} \text{ mod } 26}$$

$$= \cancel{\begin{pmatrix} 25 & 20 \\ 15 & 3 \end{pmatrix}} = \begin{pmatrix} 27 & 162 \\ 63 & 153 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} 1 & 6 \\ 11 & 23 \end{pmatrix}$$

$$KK^{-1} \bmod 26 = \begin{pmatrix} 17 & 8 \\ 19 & 3 \end{pmatrix} \begin{pmatrix} 1 & 6 \\ 11 & 23 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 105 & 286 \\ 52 & 183 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$P = CK^{-1} \bmod 26.$$

$$= (23 \;\; 2) \begin{pmatrix} 1 & 6 \\ 11 & 23 \end{pmatrix} \bmod 26 = (45 \;\; 184) \bmod 26$$

$$= (19 \;\; 2) = (T \;\; C).$$

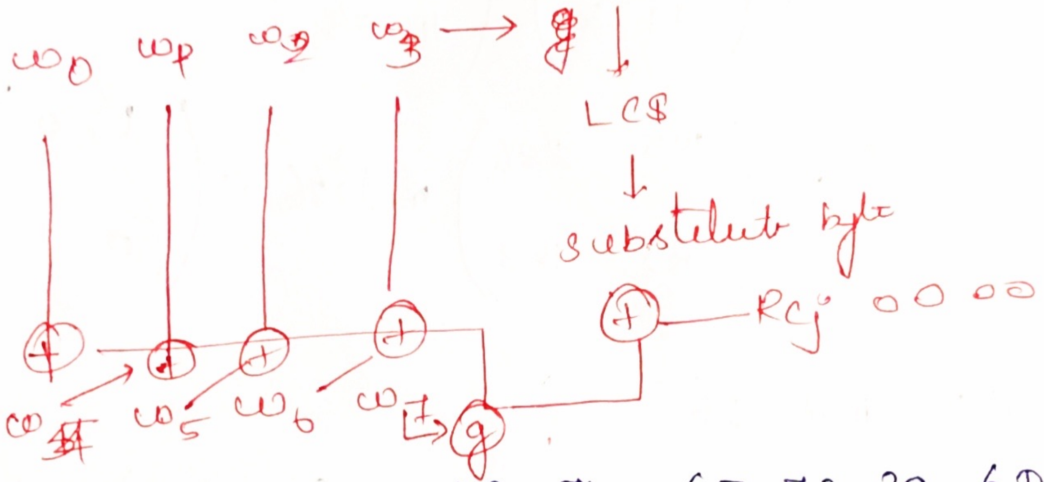
$$P = CK^{-1} \bmod 26$$

$$= (10 \;\; 16) \begin{pmatrix} 1 & 6 \\ 11 & 23 \end{pmatrix} \bmod 26 = (186 \;\; 428) \bmod 26$$

$$= (4 \;\; 12) = (E \;\; M)$$

XCKQ = TCEM

3) ii) Alg → 2 marks.



67 20 46 75 20 4B 75 6E 73 20 6D 79

54 68 61 74.

67	20	73	54
20	4B	20	68
46	75	6D	61
75	6E	79	74

wk0 wk1 wk2 wk3.

wk0 = 67 20 46 75

wk1 = 20 4B 75 6E

wk2 = 73 20 6D 79

wk3 = 54 68 61 74.

5) Elgamal.

$q = 157 \quad \alpha = 5$

i) $Y_B = 10, \quad k = 3, \quad M = 9$

$K = (Y_B)^k \bmod q = 10^3 \bmod 157 = 58$

$C_1 = \alpha^k \bmod q = 5^3 \bmod 157 = 125$

$C_2 = KM \bmod q = (58 \times 9) \bmod 157 = 51$

$C = (C_1, C_2) = (125, 51)$

ii) $M = 9$

$C = (25, C_2)$

$K = (C_1)^{X_B} \bmod q$

$Y_B = \alpha^{X_B} \bmod q.$

$10 = 5^{X_B} \bmod 157$

$C_1 = \alpha^k \bmod q$

$25 = 5^k \bmod 157$

$\boxed{k = 2}$

$K = Y_B^k \bmod q$

$= 10^2 \bmod 157$

$= 100$

$C_2 = KM \bmod q = (100 \times 9) \bmod 157 = 900 \bmod 157$

$\boxed{C_2 = 115}$

$(25, 115)$